IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO WESTERN DIVISION AT CINCINNATI

FINESSE EXPRESS, LLC and WIDER GROUP, INC, individually and on behalf of all others similarly situated, Plaintiffs, v. TOTAL QUALITY LOGISTICS, LLC, Defendant.	Case No. 20-cv-00235-MRB Honorable Michael R. Barrett

PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS THE COMPLAINT OR ALTERNATIVELY TO STRIKE CLASS ALLEGATIONS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Other Authorities

Plaintiffs Finesse Express, LLC ("Finesse") and Wider Group, Inc. ("Wider"), individually and on behalf of the putative class, (collectively, "Plaintiffs"), submit this Opposition to Defendant's Motion to Dismiss the Complaint or, in the Alternative, to Strike Class Allegations ("Def. Mtn." or "Motion") (Dkt. No. 16).

I. BACKGROUND

This is a putative class action raising claims out of a massive data security breach of the computer systems of Total Quality Logistics, LLC ("TQL" or "Defendant") that disclosed to hackers the most sensitive confidential and financial information of Plaintiffs and thousands of others. *See generally* Class Action Complaint for Damages ("Complaint") (Dkt. No. 1). Plaintiffs raise four claims for relief: negligence, breach of contract, unjust enrichment, and declaratory and injunctive relief. ¶¶ 96-141 (PageID 22-32).[1]

II. SUMMARY OF FACTUAL ALLEGATIONS

TQL is the second largest freight brokerage firm in North America. ¶ 2 (PageID 2). To facilitate its business, TQL collected Plaintiffs' and Class members' personal information, including confidential financial information. On or around February 27, 2020, Defendant announced that hackers had infiltrated its information technology ("IT") systems and had gained access to the sensitive information of Plaintiffs and the Class, including "tax ID numbers, bank account numbers, and invoice information, including amounts and dates." ¶ 17 (PageID 5). While TQL has provided little public details on the data breach, including for how long these hackers had unfettered access to the confidential information of Plaintiffs and the Class, internal sources at TQL have stated that the breach was not discovered until a TQL carrier experienced unauthorized changes to its banking information. ¶ 22 (PageID 6).

[1] All "¶" and "¶¶" references are to the Complaint unless otherwise specified.

As a result of Defendant's failure to implement adequate IT security measures that reasonably conformed with industry standards, hackers have now accessed, viewed, and, in a growing number of cases, used the unencrypted private and confidential financial information, including tax ID numbers, bank account numbers, Social Security numbers, invoice information, and other highly confidential information of Plaintiffs and the Class. ¶ 6 (PageID 3). Indeed, TQL has acknowledged that, as of February 28, 2020, nearly twenty carriers had been identified as having already experienced "ACH payment theft." ¶ 7 n.2 (PageID 3). Freight Broker Live similarly reported that, according to internal sources at TQL, several carriers' banking information had been changed and that payments were sent out to these altered bank accounts. ¶ 22 (PageID 6).

III. PLAINTIFFS HAVE ARTICLE III STANDING

To establish standing at the pleading stage, the complaint must allege facts demonstrating that the plaintiffs "have (1) suffered an injury in fact; (2) that is fairly traceable to the challenged conduct of a defendant; and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

Defendant argues that Plaintiffs fail to demonstrate two of those elements: injury-in-fact and traceability. Contrary to Defendant's contention, Plaintiffs have pled sufficient allegations to establish both elements to survive the motion to dismiss.

A. Plaintiffs Suffered Injury-In-Fact

"A party facing prospective injury has standing to sue where the threatened injury is real, immediate, and direct." *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008). Here, Plaintiffs have suffered several separate injuries that each independently confer Article III standing.

1. Injury Based on TQL's Alleged Breach of Plaintiffs' Contractual Rights

It is well-established that plaintiffs suffer an injury-in-fact where there is "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo*, 136 S. Ct. at 1548.

Here, when Plaintiffs contracted with TQL for brokerage services, the Broker-Carrier Agreement contained a material term that both parties would treat as confidential and would not disclose their personal, financial, and company information. ¶¶ 60-68, 117-124 (PageID 14-16). As such, Plaintiffs had a "legally protected" contractual right to the confidentiality of their information and to TQL's treating it as such. *See Spokeo*, 136 S. Ct. at 1548. Plaintiffs allege that they were deprived of these contractual rights when TQL breached the confidentiality provision of the contract. TQL's breach caused them injury, including the loss of the benefit of their bargain. *See, e.g.*, ¶¶ 42-49, 60-61, 128-32 (PageID 10, 14-15, 28-29).

"'[A] party to a breached contract' has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged." *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 909 (8th Cir. 2016) ("Carlsen alleged that he has suffered damages as a result of GameStop's breach in the form of devaluation of his Game Informer subscription"); *see also Ping v. Beverly Enterprises, Inc.*, 376 S.W.3d 581, 595 (Ky. 2012) (citing "general rule" that "parties to a contract may enforce or be bound by its provisions"). In other words, the violation of a private contract right is sufficient to confer standing to enforce such contract rights. *See id.*; *see also Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 716 (8th Cir. 2017) (finding injury-in-fact for the breach of a contract and resulting diminished value of the contractual right in a data breach class action); *Auto Chem Labs., Inc. v. Turtle Wax, Inc.*, No. 3:07CV156, 2010 WL 3769209, at *6 (S.D. Ohio Sept. 24, 2010) (recognizing that party to a breach of contract claim is entitled to benefit of the bargain

losses, which are "the difference in the value between what a plaintiff has received and the actual value of what he would have received if the representations had been true"); *Schambach v. Afford a Pool & Spa,* 2009 Ohio 6809, 2009 WL 4981229, at *2 (Ohio 7th App. Dist. Dec. 17, 2009) ("A party proving breach of contract is entitled to the benefit of his or her bargain."); *cf. Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring) (explaining that requirement of showing some special, concrete harm to vindicate a public wrong "does not apply as rigorously when a private plaintiff seeks to vindicate his own private rights.").

Because an injury-in-fact can exist based solely on the breach of a contractual legal right, Plaintiffs have more than sufficiently pled injury where they allege multiple additional injuries beyond just the violation of their rights. *See, e.g.*, ¶¶ 42-49, 60, 128-32 (PageID 10, 14-15, 28-29).

2. Alleged Identity Theft Constitutes Injury-In-Fact

Plaintiffs also sufficiently allege an injury-in-fact based on Plaintiff Finesse's identify theft immediately following TQL's data breach.

Plaintiffs adequately allege that their confidential financial information, including "tax ID numbers, bank account numbers, and invoice information" was compromised at the hands of TQL. ¶ 17 (PageID 5). Plaintiff Finesse further alleges that its confidential financial information was misused, and Plaintiff Finesse has identified *three fraudulent bank transactions* immediately following the data breach. ¶¶ 24, 79 (PageID 7, 18). Thus, Plaintiff Finesse has plausibly alleged that it has suffered identity theft.

The misuse of sensitive data *alone* is sufficient to confer standing. *See Resnick v. AvMed, Inc*., 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that the misuse of plaintiff's sensitive information to open a bank account was sufficient to confer standing even though she did not allege any "unreimbursed losses"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact for data breach case and defining "actual misuse" as a

"fraudulent charge"); *Burrows v. Purchasing Power, LLC*, No. 1:12-CV-22800-UU, 2012 WL 9391827, at *2 (S.D. Fla. Oct. 18, 2012) ("[A]ctual misuse even devoid of monetary loss is sufficient to confer standing…. [A] plaintiff who alleges actual identity theft without economic harm has an injury for standing"); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1317 (N.D. Ga. 2019) (rejecting notion that Plaintiffs must allege non-reimbursement, and finding that "[t]he Plaintiffs' allegations that they suffered unauthorized charges on their payment cards as a result of the Data Breach are actual, concrete injuries"). Indeed, the Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted *using the identifying information of another person without authority*." 17 C.F.R. § 248.201 (2013).[2] Thus, the unauthorized use of someone's financial information, like the fraudulent bank transactions experienced by Plaintiff Finesses, *is identity theft*.

Plaintiff Finesse clearly has injury-in-fact based on the theft of its identity to make unauthorized financial transactions.

3. Plaintiffs Have Injury-In-Fact Based on Alleged Actual Losses

Plaintiffs both alleged that, as a direct result of TQL's data breach, they have been forced to expend company time responding to the breach in an attempt to mitigate it harms.

Plaintiff Finesse alleged that it spent approximately 15 hours responding to the data breach. ¶ 78 (PageID 17). Plaintiff Finesse further alleged that it missed out on an 890-mile load worth around $2,500 that the company would have been able to secure but for the fact that Plaintiff Finesse was engaged in responding to the data breach. ¶ 80 (PageID 18). Plaintiff Wider likewise alleged that it lost company time responding to the data breach. ¶¶ 78, 81-82 (PageID 17-18).

[2] Emphasis added, and citations, internal quotations, and footnotes omitted unless otherwise noted.

Lost time and lost earnings are recognized as recoverable damages under Ohio law. Indeed, Ohio courts have historically equated "lost time" with "lost income" under the common law. *See A.F. Waite Taxi & Livery Co. v. McGrew*, 16 Ohio App. 219, 223 (1922) ("[L]oss of time and loss of earnings ordinarily mean the same thing."); *Vieira v. Addison*, No. 98-L-054, 1999 WL 689932, at *2 (Ohio Ct. App. Aug. 27, 1999) ("Compensatory damages for injuries include direct pecuniary loss, such as ... loss of time or money."). And recently, the Sixth Circuit has recognized "lost time" as recoverable damages for violations of privacy. *See Beaven v. U.S. Dep't of Justice*, 622 F.3d 540, 558-559 & n.13 (6th Cir. 2010) (concluding that lost-time damages were recoverable as "out-of-pocket" damages where plaintiff-employees' sensitive personal information had been inadvertently disclosed to inmates and other prison staff).

If plaintiffs are entitled *to recover damages* for lost time, then the loss of time is certainly sufficient to establish the less rigorous injury-in-fact requirement for standing to sue. *See McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019) ("The Plaintiffs have provided factual information that demonstrates that they have lost time and money as a result of taking steps to protect their personal data and prevent the misuse of that data by scammers. At the very least, the Plaintiffs' mitigation efforts constitute a cognizable injury that is a direct result of the unauthorized release of employees' [confidential information] by Allconnect").

Indeed, courts across the country have held that the loss of time spent responding to data breaches is sufficient to establish an injury-in-fact in consumer class actions. *See, e.g.*, *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018) ("the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective"); *Pedro v. Equifax, Inc.*, 868 F.3d 1275, 1280 (11th Cir. 2017) (holding that FCRA plaintiff had "alleged a concrete injury because she alleged that she 'lost time . . . attempting to resolve the credit inaccuracies'"); *Sisley*

v. Sprint Comm'ns Co., L.P., 284 Fed. Appx. 463, 466 (9th Cir. 2008) (finding "cognizable injury in fact" based on allegations of lost time); *In re General Motors LLC Ignition Switch Litig.*, 339 F. Supp. 3d 262 (S.D.N.Y. 2018) (concluding that loss of personal time constituted damages for breach of contract and other claims in consumer class action).

Because injury-in-fact exists for consumers spending their personal time responding to a data breach, such injury is even more evident when a *company* is required to spend *staff* time reviewing accounts, calling banks, disputing transactions, and otherwise responding to a data breach, as is the case here. ¶¶ 78-82 (PageID 17-18). Thus, Plaintiffs' loss of time confers standing.

4. Plaintiffs Allege Injury-in-Fact Based on the Substantial Risk of Future Harm

An allegation of threatened injury in the future is sufficient to establish standing "if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). Supreme Court precedent does not "uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about"—hence, the "substantial risk" standard. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013). Ultimately, the purpose of the imminence requirement is "to ensure that the court avoids deciding a purely hypothetical case in which the projected harm may ultimately fail to occur." *Baur v. Veneman*, 352 F.3d 625, 632 (2d Cir. 2003).

Applying these principles in the context of a data breach case, the Sixth Circuit case in *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) explained:

> There is *no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals*. Indeed, [the defendant] seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year. *Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints*.

> Thus, although it might not be "literally certain" that Plaintiffs' data will be misused, *there is a sufficiently substantial risk of harm* that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, particularly when [the defendant] recommended taking these steps. And here, the complaints allege that Plaintiffs and the other putative class members must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts.

Id. at 388-89.

The Sixth Circuit's holding is consistent with that of many courts that have found standing based on an increased risk of future identity theft. *See, e.g.*, *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) (holding that victims of a data breach had established injury-in-fact by alleging a "substantial risk of harm" from the theft of their data, wherein the court explained: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make a fraudulent charge or assume those consumers' identities."); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir.2010) (finding "increased risk of future identity theft" sufficient to confer standing, holding that "[i]f a plaintiff faces 'a credible threat of harm' and that harm is 'both real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III."); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017) ("The principal question, then, is whether the plaintiffs have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have.").

TQL's strained suggestion that the data breach did not disclose information that would be useable to identity thieves is wholly implausible and unpersuasive. TQL's notification to Plaintiffs stated that the data breach compromised Plaintiffs' "tax ID number[s], bank account numbers, and invoice information…." ¶ 17 (PageID 5). It is reasonable to conclude that "invoice information" included names or other identifying information, particularly since TQL's email further advised

Plaintiffs to "contact your financial institution immediately, letting them know your bank information has been exposed." ¶ 19 (PageID 5). If the exposed information were truly unusable, TQL would have no cause to make this recommendation. Indeed, the fact that TQL gave any notification of the data breach suggests that the breach must have exposed usable confidential information since Ohio law only requires notification of a data breach when it is "reasonably believed to have caused, or reasonably is believed *will cause a material risk of identity theft* or other fraud to the person or property." Ohio Rev. Code § 1349.19(A)(1)(a). And importantly, TQL has admitted that its data breach *has resulted* in several of its carriers *actually experiencing "ACH payment theft."* ¶¶ 7 n.2, 22 (PageID 3, 6).[3] Moreover, Plaintiff Finesse experienced actual identity theft in the form of fraudulent bank transactions as a result of TQL's data breach. All of these facts wholly undermine the validity of TQL's argument in its Motion. Thus, while it is true that TQL has provided intentionally vague details to the victims of its data breach, this self-serving tactic does not insulate TQL from liability for the injuries it caused.

While TQL also cites *Galaria* to argue that a substantial risk of harm must be coupled with reasonably incurred mitigation costs (Def. Mtn. at 7), this argument is unpersuasive. First, *Galaria* did *not* hold that mitigation costs are required; instead, the Court recognized that "a 'substantial risk' that the harm will occur, which *may* prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," is sufficient to establish injury-in-fact. 663 F. App'x at 388. Second, even were mitigation costs necessary, this is of little import here since Plaintiffs *do* allege they incurred such mitigation costs. ¶¶ 78-82 (PageID 17-18). Notably, Plaintiffs allege that they suffered costs in the form of lost company time spend in an attempt to mitigate the effects of the theft, and courts,

[3] It is truly unclear how TQL can simultaneously admit that the data breach caused actual electronic payment theft while arguing that the exposed financial information did not include enough information for a payment fraud to occur.

including those interpreting Ohio law, recognize such loss of time to be a compensable injury. *See supra* Section III.A.3. In fact, *Galaria* itself recognizes that the loss of time constitutes an injury. 663 F. App'x at 388 ("Plaintiffs and the other putative class members must expend *time* and money to monitor their credit, check their bank statements, and modify their financial accounts.").

Plaintiffs, whose confidential information was compromised in TQL's data breach, have established a substantial risk of harm and, therefore, have standing to bring claims against TQL.

5. Injury Based on Depreciation of Value of Personal Information

Plaintiffs allege the intrinsic value of their confidential information has been diminished by the TQL data breach. ¶ 47 (PageID 11-12).

These allegations of injury arising from the loss of value of confidential information are sufficient to confer Article III standing. For example, in *In re Facebook Privacy Litigation*, 572 Fed. Appx. 494 (9th Cir. 2014), the court found plaintiffs plausibly alleged they experienced harm where the plaintiffs' confidential information was disclosed in a data breach, and the plaintiffs "los[t] the sales value of th[eir] [personal] information" as a result. *Id.* Similarly, in *In re Marriott Interntional, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 869241 (D. Md. Feb. 21, 2020), the court correctly reasoned: "Neither should the Court ignore what common sense compels it to acknowledge – the value that personal identifying information has in our increasingly digital economy." *Id.* at *8. Additionally, in *In re Anthem, Inc. Data Breach Litigation* ("*Anthem II*"), 2016 WL 3029783 (N.D. Cal. May 27, 2016), the court found plaintiffs plausibly alleged injury from the loss of value of their confidential information, explaining that, for standing purposes, a plaintiff must "allege that there was either an economic market for their [personal information] *or* that it would be harder to sell their own [personal information], not both." *Id.* at *14-15; *see also Svenson v. Google, Inc.*, 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015)

("Svenson's allegations of diminution in value of her [confidential information] are sufficient to show contract damages for pleading purposes.").

While Defendant argues that Plaintiffs must demonstrate that they intended to sell their confidential information to establish injury, this argument lacks logical sense, as courts have recognized. In *In re Marriott Interntional, Inc., Customer Data Sec. Breach Litig.*, the court held:

> [T]he value of consumer personal information is not derived solely (or even realistically) by its worth in some imagined market place where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check.

2020 WL 869241 at *9; *see also Svenson*, 2015 WL 1503429, at *5 (holding that plaintiffs are not required to plead that they intended to sell their own confidential information); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) (same).

Plaintiffs alleged: that their confidential information (including financial information) is a valuable commodity (¶¶ 31-49, Page ID 8-12), a fact that Defendant recognizes (¶ 49, PageID 12); that a market exists for Plaintiffs' confidential information, (¶ 47, PageID 11); that as a result of the Data Breach, their confidential information was compromised by hackers, (¶¶ 28-56, PageID 7-14) and; that their confidential information lost value as a result, particularly as to Plaintiff Finesse who experienced fraudulent bank transactions (¶¶ 43-47, PageID 9-12). These allegations are sufficient to allege injury for standing purposes.

B. Plaintiffs' Injuries are Fairly Traceable to Defendants' Wrongdoing

The allegations in the Complaint easily meet the second requirement for standing—a causal connection showing that the injury is fairly traceable to Defendant's actions. "A showing that an injury is 'fairly traceable' requires less than a showing of 'proximate cause.'" *Resnick*, 693 F.3d at 1324; *see Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014).

"[S]howing that a plaintiff's injury is *indirectly* caused by a defendant's actions satisfies the fairly traceable requirement." *Resnick*, 693 F.3d at 1324.

In *Galaria*, the Sixth Circuit found traceability met in the context of a data breach. The Court held that "but for [the defendant's] allegedly lax security, the hackers would not have been able to steal Plaintiffs' data. These allegations meet the threshold for Article III traceability, which requires more than speculative but less than but-for causation." 663 F. App'x at 390.

Plaintiffs' allegations are substantially similar to those addressed in the *Galaria* decision. Plaintiffs allege they provided their confidential information to TQL, and both Plaintiffs received notifications from TQL that their confidential financial information was compromised in the data breach. ¶¶ 16-19 (PageID 5). While Defendant again argues that there was not enough information exposed in the data breach to be used in an identity theft, Plaintiffs addressed these specious arguments *supra* at Section III.A.4. Quite simply, the injuries discussed *supra* each derived from TQL's inadequately-secured IT system that exposed Plaintiffs' confidential information. Thus, Plaintiffs' allegations are sufficient to "fairly trace" their alleged injuries to Defendant's failures.

C. Plaintiffs Have Standing to Seek Injunctive Relief

To establish "injury in fact" for purposes of injunctive relief, a plaintiff must show that "if unchecked by the litigation, the defendant's allegedly wrongful behavior will likely occur or continue, and that the threatened injury is certainly impending." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 190 (2000).

Plaintiffs allege that TQL failed to implement the reasonable industry standards that were necessary to protect Plaintiffs' confidential information from preventable hack and data breach. ¶¶ 55-59 (PageID 14). Plaintiffs further allege that TQL breached the TQL-drafted Broker/Carrier Agreement ("BCA"), executed between TQL and Plaintiffs. The BCA provides:

> If *confidentiality is breached*, the Parties agree that the remedy at law, including monetary damages, may be inadequate and that *the Parties shall be entitled*, in addition to any other remedy available, *to an injunction restraining the violating Party from further violation* of this Agreement."

¶ 61 (PageID 15). Here, Plaintiffs allege that TQL has already breached their confidential information and lacks the necessary tools to comply with the confidentiality provision. Thus, it is for precisely for this kind of circumstance that the BCA contemplates a right to an injunction.

Plaintiffs allege that they risk actual or threatened injury with a reasonable probability. TQL still retains the confidential information of Plaintiffs. ¶ 48 (PageID 12). According to Plaintiffs, TQL failed to comply with the reasonable industry standards that were necessary to prevent a data breach, including encryption, segmented networks so that cyber intruders would not be able to access and extract Plaintiffs' confidential information, and firewalls so that cyber intrusions would be detected. ¶¶ 55- 58, 71-76 (PageID 14, 17); *see also* ¶ 22 (PageID 6).

Instead of arguing that it has taken all necessary precautions, TQL rejects that the tools necessary to protect the confidential information are actually necessary. In its Motion, TQL admits that it does not believe it is required to implement reasonable industry standards to protect Plaintiffs' confidential information. *See* Def. Mtn. at 20 (PageID 121) (referring to the data security policies, rules, and procedures that are reasonably necessary to protect the confidential information and stating "the BCA does not obligate TQL to 'implement' any of these measures"). TQL even claims that the confidentiality provision imposes no obligation upon it to "protect the Confidential Information of Plaintiffs and the Class." *Id.* Under these circumstances, Plaintiffs have plausibly alleged that without an injunction they face a significant risk of being harmed again from TQL's inadequately secure IT system that still contains their confidential information. Likewise, Plaintiffs have plausibly alleged that they are entitled to an injunction as a matter of contractual right. ¶ 61 (PageID 15).

Because Plaintiffs demonstrate that the "allegedly wrongful behavior will likely occur or continue," Plaintiffs have standing to bring their claim for injunction. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1161 (D. Minn. 2014) ("[Defendant's] arguments regarding Plaintiffs' standing are premature. Plaintiffs have plausibly pled that their injuries will be redressed by the injunctive relief they seek, and at this stage, that is all that is required.") (discussing Supreme Court cases where injunctive standing was found based on less certain impending injuries).

IV. PLAINTIFFS STATE CLAIMS ON WHICH RELIEF CAN BE GRANTED

A. Ohio Law Governs Plaintiffs' Claims

Defendant dedicated a full page to argue that Ohio law applies, and it then used four pages in its Motion to Strike Class Allegations to argue that class-treatment is improper because multiple state laws apply. *Compare* Def. Mtn. at 18-19 (PageID 119-20) *with id.* at 34-37(PageID 135-38). Plaintiffs have resolved this debate before and can do so again: "Plaintiffs . . . are not seeking the application of varied and inconsistent laws from across jurisdictions." *See* Dkt. No. 14 at 4-5 (PageID 93-94). Both Plaintiffs and Defendants agree that the express choice-of-law provision for Ohio law applies to all common law claims between Plaintiffs and the class and TQL. *See* Def. Mtn. at 18 (PageID 119); *infra* Section V.A.

B. The Complaint Satisfies the Pleading Standard

A complaint will survive a Rule 12(b)(6) motion when it contains "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In ruling on a motion to dismiss, the Court must "construe the complaint in the light most favorable to the plaintiff, accept its allegations as true, and draw all reasonable inferences in favor of the plaintiff." *Cates v. Crystal Clear Techs., LLC*, 874 F.3d 530, 534 (6th Cir. 2017) (quoting *Bickerstaff v. Lucarelli*, 830 F.3d 388, 396 (6th Cir. 2016)).

C. Plaintiffs' Breach of Contract Claim Is Sound

Plaintiffs' allegations are sufficient to meet the elements required for a breach of contract. Taking as true all allegations, the Court should deny Defendant's attempt to dismiss Plaintiffs' breach of contract claim.

"In order to substantiate a breach of contract claim in the state of Ohio, a party must establish the following four elements: (1) a binding contract or agreement was formed; '[(2)] the nonbreaching party performed its contractual obligations; [(3)] the other party failed to fulfill its contractual obligations without legal excuse; and [(4)] the nonbreaching party suffered damages as a result of the breach.'" *Carbone v. Nueva Constr. Grp., L.L.C.*, 83 N.E.3d 375, 380 (Ohio Ct. App. 2017) (citing *Textron Fin. Corp. v. Nationwide Mut. Ins. Co.*, 115 Ohio App.3d 137, 144, 684 N.E.2d 1261 (Ohio Ct. App. 1996)).

While there is no dispute as to whether a contract between TQL and Plaintiffs was formed, TQL argues that there was no breach of the contract because, according to TQL, its terms did not expressly obligate TQL to protect Plaintiffs' confidential information from hackers. This is simply not true.

The BCA was comprised of a set of promises, each of which are actionable upon a breach thereof. One such promise that TQL made expressly in the contract includes the following promise to maintain Plaintiffs' information as confidential:

> **CONFIDENTIALITY.** In addition to confidential information protected by law, whether statutory or otherwise, the Parties agree that all of their ***financial information*** and that of CUSTOMERS, including, without limitations, freight and brokerage rates, amounts received for brokerage services, amounts of freight charges collected, amounts of freight charges paid, freight volume requirements, as well as related CUSTOMER information, CUSTOMER shipping or other logistic requirements shared or learned between the Parties and CUSTOMERS ***shall be treated as confidential, and shall not be disclosed*** or used for any reason without prior written consent by the Parties. ***If confidentiality is breached***, the Parties agree that the remedy at law, including monetary damages, may be inadequate and that

> the Parties shall be entitled, in addition to any other remedy available, to an injunction restraining the violating Party from further violation of this Agreement.

¶ 61 (PageID 15) (emphasis added).

This express term of confidentiality provides that Plaintiffs' information "shall be treated as confidential, and shall not be disclosed or used for any reason without prior written consent." It is impossible for information to be "treated as confidential" when TQL's inadequate system permits an unauthorized third-party to access that information. It is also impossible for information to "not be disclosed" without prior written consent when it is in the hands of hackers and identity thieves. Under the contract, it was TQL's duty to maintain confidentiality and take reasonable steps to prevent Plaintiffs' confidential information from *not* being treated as confidential and from *not* being "disclosed." It failed to do both.

The words "shall not be disclosed" are particularly problematic for TQL as courts have interpreted the word "disclose" to apply to situations of security breaches. In *Beaven v. U.S. Dep't of Justive*, No. CIV.A.03 84 JBC, 2007 WL 1032301 (E.D. Ky. Mar. 30, 2007), *aff'd in part, rev'd in part and remanded sub nom. Beaven v. U.S. Dep't of Justice*, 622 F.3d 540 (6th Cir. 2010), the Court held that the defendants violated the Privacy Act, 5 U.S.C. § 552a(b), which provides that "[n]o agency shall *disclose* any record…," where a prison employee inadvertently left a folder containing confidential employee information on a desk where inmates were able to access it. *Id.* at *17. This holding was sustained on appeal where the Sixth Circuit further affirmed that the *disclosure* was "intentional or willful" even though the employee's final act of leaving the folder unsecured was "inadvertent." *Beaven v. U.S. Dep't of Justice*, 622 F.3d 540, 544 (6th Cir. 2010). Certainly here then, Plaintiffs have plausibly alleged that TQL violated its contractual obligation not to "disclose" Plaintiffs' confidential information based on TQL's inadequate security measures

and systems. ¶¶ 55-76 (PageID 14-17). To be sure, the words "shall not be disclosed" can include *negligent* disclosure.

Even if this Court were to find that TQL did not "disclose" Plaintiffs' confidential information, the operative words "if confidentiality is breached" are unavoidable to Defendant. This sentence of the confidentiality clause (which TQL drafted) does not say "if information is disclosed…" but instead specifically contemplates a "breach[]" of the confidentiality. As such, Plaintiffs' loss of the expressly promised and contractually bargained-for confidentiality of their sensitive information, whether negligently disclosed or accessed in a security breach, is sufficient to serve as a breach of the BCA's terms by TQL.

To the extent there is any ambiguity in the contract, such ambiguity must be interpreted in favor of Plaintiffs. *See Westgate Ford Truck Sales v. Ford Motor Co.*, 25 N.E.3d 410, 414-15 (Ohio Ct. App. 2014) ("A contract is ambiguous when it is susceptible to more than one reasonable interpretation."). "Where the written contract is standardized and between parties of unequal bargaining power, an ambiguity in the writing will be interpreted strictly against the drafter and in favor of the non-drafting party." *Westfield Ins. Co. v. Galatis*, 797 N.E.2d 1256, 1262 (Ohio 2003); *see also In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 WL 539578, at *10-11 (D. Or. Feb. 9, 2017) (denying the motion to dismiss the breach of contract claim and finding that "any ambiguities must be construed against Defendant"). Here, because TQL drafted the contract, any ambiguous terms, including those within the confidentiality clause of the BCA, are to be read in favor of the Plaintiffs. Thus, because the BCA can reasonably be interpreted as obligating TQL to use reasonable measures to securely maintain Plaintiffs' confidential information free from disclosure or breach, the BCA *must* be interpreted this way.

In the context of data breach cases, courts have held companies liable for breach of contract claims that are based on less specific provisions than those present here. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, at *44 (finding breach of contract alleged where Terms of Service stated, *inter alia*: "We are committed to ensuring your information is protected and apply safeguards in accordance with applicable law," and "We limit access to personal information about you to employees who we reasonably believe need to come into contact with that information to provide products or services to you or in order to do their jobs."); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *5 (S.D. Cal. May 7, 2020) (finding breach of contract claim pled based on website policies that state: "Solara Medical Supplies...is committed to protecting your privacy and understands the importance of safeguarding your personal health information" and "[a]s our client you have the right to ... Confidentiality of your records"); *Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 759 (W.D.N.Y. 2017) (finding breach of contract alleged where privacy notices attested to safeguard personal information and assured that "all systems that contain personal information have security protections"); *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 801-02 (W.D. Wis. 2019) (finding breach of contract sufficiently alleged where privacy policy promised to store patient information in a "secure database."); *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, 2017 WL 539578, at *11 & *16 (finding breach of contract sufficiently pled where the privacy notice noted Defendant's commitment to protect and safeguard the private information of its customers).

Because Plaintiffs have plausibly alleged that TQL failed to fulfill its contractual obligation to maintain the confidentiality of Plaintiffs' sensitive information, the Court should deny Defendant's attempt to dismiss Plaintiffs' breach of contract claim.

D. Plaintiffs Plead Actionable Negligence Claims

Plaintiffs' claims fall within two well-established exceptions to the so-called economic loss rule. First, Plaintiffs allege non-economic harm. Second, TQL has a duty to Plaintiffs independent of any contract.

1. The Economic Loss Doctrine Does Not Apply

a. Plaintiffs Allege Non-Economic Harm

The economic loss rule does not apply when both economic and non-economic losses are alleged. *See Lifelink Pharm., Inc. v. NDA Consulting, Inc.*, No. 5:07-CV-785, 2007 WL 2292461, at *4 (N.D. Ohio Aug. 7, 2007) ("Ohio's economic-loss rule typically prevents a plaintiff who has suffered *only* economic losses from recovering tort damages.") (finding economic loss doctrine inapplicable where plaintiff "alleged at least two injuries beyond mere economic loss"). In *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024 (N.D. Cal. 2019), a data breach case, the court explained that the plaintiff's allegation of lost time is non-economic and, therefore, the economic loss rule "does not apply." *Id.* at 1039; *see, e.g., In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020).

Here, similarly, Plaintiffs have alleged their loss of time and other losses beyond mere economic loss. ¶¶ 78-81 (PageID 17-18). Such allegations for lost time have been found to constitute a cognizable and concrete injury. *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388–89 (6th Cir. 2016) ("[T]he complaints allege that Plaintiffs and the other putative class members must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts. … these costs are a concrete injury suffered to mitigate an imminent harm…."); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019) ("The Plaintiffs have provided factual information that demonstrates that they have lost time and money as a result of taking steps to protect their personal data and prevent the misuse of that data

by scammers. At the very least, the Plaintiffs' mitigation efforts constitute a cognizable injury that is a direct result of the unauthorized release of employees' [confidential information] by Allconnect").

Accordingly, because Plaintiffs allege both economic and non-economic losses, the economic loss rule does not apply.

b. TQL Owed Plaintiffs an Independent Duty in Tort

"[W]here a tort claim alleges that a duty was breached independent of the contract, the economic loss rule does not apply." *Ineos USA LLC v. Furmanite Am., Inc.*, 2014 WL 5803042, at *6 (Ohio Ct. App. Nov. 10, 2014); *see also In re Nat'l Century Fin. Enterprises, Inc.*, 504 F. Supp. 2d 287, 325 (S.D. Ohio 2007). Indeed, "the economic-loss rule does not apply—and the plaintiff who suffered only economic damages can proceed in tort—if the defendant breached a duty that did not arise solely from a contract." *Mulch Mfg., Inc. v. Advanced Polymer Sols., LLC*, 947 F. Supp. 2d 841, 856 (S.D. Ohio 2013) (quoting *Campbell v. Krupp*, 195 Ohio App.3d at 580, 961 N.E.2d 205 (Ohio Ct. App. 2011)); *see Davis v. Venture One Const., Inc.*, 568 F.3d 570, 577 (6th Cir. 2009) ("Just because a person acts pursuant to a contract does not mean other common law duties disappear."). In other words, where a defendant has a legal duty that is independent of any contract, the plaintiff can maintain a separate tort claim.

Here, TQL has an independent duty to handle its motor carriers' and customers' confidential information with due care and consistent with industry standards to prevent the foreseeable harm that arises from a breach of that duty. The overwhelming majority of courts, including courts within this Circuit, have recognized such a duty. *See Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-00186-TBR, 2017 WL 5986972, at *3, 9 (W.D. Ky. Dec. 1, 2017) (data breach plaintiffs sufficiently alleged defendant breached a duty owed to them). For example, in *McKenzie*

v. Allconnect, Inc., 369 F. Supp. 3d 810 (E.D. Ky. 2019), the court considered arguments similar to those raised by TQL and held that an independent duty of care exists:

> [W]hen accepting the facts as true and reading the complaint in the light most favorable to the Plaintiffs, the Plaintiffs have provided sufficient information at this stage to survive a motion to dismiss on the duty of care element. The Plaintiffs have provided sufficient information in the complaint to demonstrate that *they were obligated to provide sensitive personal information to Allconnect as a condition of their employment*. As a result, while Allconnect may not have had a duty to protect to its employees from unknown or unforeseen third-parties, *Allconnect did have a duty to prevent foreseeable harm to its employees and, as part of that duty, had a duty to safeguard the sensitive personal information of its employees from unauthorized release or theft*.

Id. at 817-18. This is consistent with findings of many courts holding that an independent duty exists to protect sensitive information. *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 968 (S.D. Cal. 2014) ("[Defendant] owed [p]laintiffs a legal duty to provide reasonable network security. . . , which was separate and independent from the [contract]"); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1326 (N.D. Ga. 2019) ("Defendants owed a legal duty [in tort] to take reasonable measures to prevent a reasonably foreseeable risk of harm due to a data breach incident."); *In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 799 (N.D. Cal. 2019); *In re Arby's Rest. Grp. Inc. Litig.*, 2018 WL 2128441, at *13 (N.D. Ga. Mar. 5, 2018); *In re Marriott Int'l, Customer Data Sec. Breach Litig.*, 2020 WL 869241, at *20 (D. Md. Feb. 21, 2020); *see also Savidge*, 2017 WL 5986972, at *9 (W.D. Ky. Dec. 1, 2017) ("The employees provided their personal information for tax purposes and to receive employment and benefits, with the understanding that Seagate, while it held the information, would take adequate measures to protect it…. [I]t is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently.").

Here, TQL solicited, gathered, and stored the sensitive confidential information of Plaintiffs and the Class. ¶ 4 (PageID 2). TQL had an independent duty to reasonably safeguard that confidential information, including from the preventable and foreseeable criminal conduct of third parties. ¶¶ 50- 59, 68-76 (PageID 12-14, 16-17); *see also* Restatement (Second) of Torts § 302B. It was foreseeable that injury to Plaintiffs and the Class would result from Defendant's violation of its duties in mishandling the confidential information of Plaintiffs and the Class. *Id.*; ¶¶ 31-49 (Page ID 8-12). Because Plaintiffs have sufficiently stated a claim for Defendant's tort duty independent from any contract, the economic loss doctrine does not apply.

Further, Defendant argues that the contract does not obligate TQL to actively protect class members' confidential information and/or to maintain adequate security measures. Def. Mtn. at 20 (PageID 121). Thus, under Defendant's stated position, Plaintiffs' allegations that TQL failed to protect Plaintiffs' confidential information by implementing and maintaining adequate data security protocols and measures must be viewed as an alleged violation of a duty in tort, not a duty in contract. While Plaintiffs disagree with Defendant's interpretation of the contract between Plaintiffs and TQL, the very fact that there is a dispute on the issue supports allowing the negligence claim to proceed. *See Ineos USA LLC v. Furmanite Am., Inc.*, 2014 WL 5803042, at *7 (Ohio Ct. App. Nov. 10, 2014) ("So long as there is a legitimate dispute as to what duties the contract created, we cannot adequately determine whether the tort alleges a breach of the same duties.").

2. Plaintiffs Plausibly Allege that Defendant Breached Its Duty

Plaintiffs allege that TQL breached its duty to protect confidential information entrusted to it in the face of preventable and foreseeable risks by, among other things, failing to maintain adequate IT systems and data security practices to safeguard Plaintiffs' confidential information and by failing to comply with the minimum industry data security standards, including the FTC guidelines. ¶¶ 55-

58, 71-76 (PageID 14, 17). Indeed, Plaintiffs allege that Plaintiffs' tax identification numbers, bank account numbers, invoice information, and other confidential information were captured through the data breach. ¶ 17 (PageID 5). Had TQL properly segmented its network, the cyber intruders would *not* have been able to access and extract the valuable confidential information of TQL's customers undetected. ¶ 73 (PageID 17). Similarly, had TQL utilized industry standard encryption to store its customers' confidential information, such information would *not* have been legible or comprehensible to outside hackers. ¶ 72 (PageID 17). *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (holding plaintiffs had alleged breach of duty to provide reasonable security by pleading that defendant failed to employ reasonable security measures to protect the information, including failing to use industry standard encryption); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 16-CV-0014, 2016 WL 6523428, at *11 (S.D. Cal. Nov. 3, 2016) ("Because Plaintiff alleges that he provided his [confidential information] to Defendants as part of a commercial transaction, and that Defendants failed to employ reasonable security measures to protect such [confidential information], such as the utilization of industry-standard encryption, the Court finds that Plaintiff has sufficiently alleged a legal duty and a corresponding breach[.]"). Moreover, had TQL utilized effective firewalls, the data breach would not have gone undetected for "quite a while" until a carrier notified TQL of suspicious activity in its accounts. ¶ 22 (PageID 6).

Indeed, "[h]ere, the Court can draw the reasonable inference that, because Plaintiffs' information was released to unauthorized individuals, Defendants breached their duties to safeguard that information." *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-00186-TBR, 2017 WL 5986972, at *3 (W.D. Ky. Dec. 1, 2017); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019)

(finding negligence claim sufficiently pled based on allegations of unauthorized use of plaintiffs' personal information).

While Defendant claims that Plaintiffs' allegations of breach are "insufficient" (Def. Mtn. at 24, PageID 125), Defendant's position requires too much. Plaintiffs are required only to allege a "plausible" claim that Defendant breached a duty owed to Plaintiffs. *Iqbal*, 556 U.S. at 663. Although TQL has not disclosed many details about the breach, Plaintiffs allege claims that are certainly plausible: Plaintiffs allege "enough fact to raise *a reasonable expectation* that discovery will reveal evidence" to support Plaintiffs' claims. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007); *see In re Arby's Rest. Grp. Inc. Litig.*, 2018 WL 2128441, at *10 ("The parties disagree on the facts relevant to the breach and the adequacy of Defendant's precautionary measures…. *These types of disputes are improper for resolution on a motion to dismiss when Plaintiffs' factual allegations are accepted as true*."). Defendant's attempt to hold the relevant details close to the vest and then rachet up Plaintiffs' pleading burden to fact pleading is contrary to law and should be rejected. *See Gross v. Nationwide Credit, Inc.*, No. 1:10-CV-00738, 2011 WL 379167, at *3 (S.D. Ohio Feb. 2, 2011) ("The federal rules still provide for notice pleading, *not fact pleading*, and *Iqbal* and *Twombly* did not rewrite the rules. . . . *Iqbal* and *Twombly* slightly narrowed the field to complaints that set forth plausible, not merely possible, claims."). Defendant's speculation that even a company using every reasonable precaution could conceivably still experience a data breach does not make Plaintiffs' claims any less plausible—particularly here where if TQL had utilized industry standard encryption, the confidential information would have been indecipherable. In truth, the debate about whether TQL's security measures were in fact negligently inadequate is premature at this stage. "Whether Plaintiffs can *prove* such a breach is matter reserved for summary judgment or trial. However, at this early stage, it

is enough that Plaintiffs have plausibly alleged a breach of Defendants' duties." *Savidge*, 2017 WL 5986972, at *3 (W.D. Ky. Dec. 1, 2017) (emphasis in original).

3. Plaintiffs Allege Proximate Causation

To sufficiently plead proximate causation, Plaintiffs need only allege "a plausible causal relationship between [the] alleged negligence and plaintiffs' injuries." *Brown v. Whirlpool Corp*., 996 F. Supp. 2d 623, 637 (N.D. Ohio 2014). Plaintiffs readily meet that standard here.

Plaintiffs allege that they were required to provide their tax identification numbers, bank account numbers, and other confidential information. ¶ 4 (PageID 2). Plaintiffs allege that Defendant negligently failed to implement and maintain reasonable security measures to protect Plaintiffs' and class members' confidential information. ¶¶ 50- 59, 68-76 (PageID 12-14, 16-17). Defendant acknowledges that cyber criminals gained access to Plaintiffs' confidential information *by infiltrating Defendant's systems*, which has exposed Plaintiffs' and class members' confidential information to actual and potential fraud. ¶¶17, 19, 22 (PageID 5-6). Plaintiffs allege that the unauthorized exposure of their confidential information has caused them injuries in the form of, among other things: lost time responding to the data breach (¶¶ 78-81, PageID 17-18); diminution in the value of their confidential information and lost benefit of their bargain (¶¶ 31-49, 131; PageID 8-12, 29); and, in the case of Plaintiff Finesse, *three* fraudulent transactions that occurred between late February and March 16, 2020 (*i.e.*, within one month's time following the data breach) (¶¶ 24, 79; PageID 7, 18). Accordingly, Plaintiffs have at least alleged "a plausible causal relationship between [TQL's] alleged negligence and plaintiffs' injuries." *Brown*, 996 F. Supp. 2d at 637; *see, e.g., McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019) (finding causation for negligence claim where, as here, "there is no dispute that an unauthorized data release occurred in this case that resulted in Plaintiffs' personal information being released to unknown third-parties").

While Defendant insists that "'to prove that a data breach caused identify theft, the pleadings must include allegations of a nexus between the two instances,'" Def. Mtn. at 25 (quoting *Resnick v. AvMed, Inc*, 693 F.3d 1317 (11th Cir. 2012)), Defendant's argument misses the point.

First, although certain allegations may facilitate pleading a plausible connection between a data breach and a particular identity theft, Plaintiffs allege that Defendant's negligence proximately caused *multiple* forms of harm, only one of which is identity fraud. ¶¶ 46-47 (PageID 10-12). Plausibly alleging proximate causation for these *other* categories of harm does not require alleging a "nexus" between the TQL data breach and an identity theft. Instead, for example, Plaintiffs allege a plausible causation relationship between the TQL data breach and Plaintiffs' lost time in responding to the data breach by alleging that Plaintiffs were notified that their confidential information was exposed in the data breach, and in response, Plaintiffs devoted time to addressing the breach in an attempt to mitigate the harm it would cause them. ¶¶ 78-81 (PageID 17-18); *see Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 696 (7th Cir. 2015) ("It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level.").

Second, the Complaint in fact includes allegations sufficient to connect the TQL data breach to three fraudulent charges experienced by Plaintiff Finesse within *one month* of Plaintiff Finesse's confidential information being exposed by TQL. Accordingly, Defendant's reliance on *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-CV-118, 2017 WL 4987663 (S.D. Ohio Aug. 16, 2017) is unpersuasive. In *Galaria*, the plaintiff's alleged attempted identity fraud did not take place for more than one year after the data breach occurred—not within a few days to four weeks of the data breach, as here (¶¶ 16, 24, 79; PageID 5, 7, 18). *Id.* at *7. Indeed, Plaintiff Finesse's

allegations are stronger than those in *Resnick*, a case upon which Defendant relies. In *Resnick*, two laptops containing the defendant's customers' sensitive information were stolen from the defendant's office. 693 F.3d at 1322. Ten months after the theft, two of the defendant's customers (the plaintiffs) had their sensitive information used to open bank accounts and make unauthorized purchases. *Id.* The Eleventh Circuit held that the plaintiffs' claims could survive, despite a ten-month gap between the breach and the data being compromised, because the information stolen was the same information needed to open bank accounts in the customers' names, satisfying the logical connection. *Id*. at 1327. Such a leap is not even necessary here, given that Plaintiff Finesse experienced three fraudulent charges requiring the compromised information within just one month of the TQL data breach. ¶¶ 16, 24, 79 (PageID 5, 7, 18). *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1318 (N.D. Ga. 2019) ("Many of the Plaintiffs have alleged in the Complaint that they suffered some form of identity theft or other fraudulent activity as a result of the Data Breach. Such an allegation is sufficient at the pleading stage to establish that the Data Breach was the proximate cause of this harm."). Further, to the extent Defendant argues that the Complaint is insufficient because it failed to allege that Plaintiffs' injuries were not the result of other possible breaches, courts have correctly recognized that "[t]he Plaintiffs need not explicitly state that other breaches did *not* cause these alleged injuries, since their allegations that this Data Breach *did* cause their injuries implies such an allegation.") (emphasis in original). Indeed, Defendant's challenges to proximate causation are especially specious here since TQL has acknowledged that its data breach resulted in several of its carriers experiencing "ACH payment theft." ¶¶ 7 n.2, 22 (PageID 3, 6).

To the extent there is any question as to proximate causation, the question is one to be resolved by the fact finder. *In re Nat'l Prescription Opiate Litig.*, 2020 WL 871539, at 13 (N.D.

Ohio Feb. 21, 2020) ("Ordinarily, the existence of proximate cause is a question of fact to be determined by the trier of fact.") (citing *Strother v. Hutchinson*, 423 N.E.2d 467, 471 (Ohio 1981)); *see also In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1319 (N.D. Ga. 2019) (holding that defendant's causation arguments merely raised "a dispute of fact that is not appropriate for resolution at this stage of the litigation").

4. Plaintiffs Allege Damages Sufficient to State a Negligence Claim

Plaintiffs plausibly allege that they were damaged as a result of the TQL data breach.

Each Plaintiff articulated specific non-general damages in their costs and loss of company time caused by the data breach, including time spent. Indeed, both Plaintiffs incurred notable time and cost reviewing transactions on their company bank accounts, time spent reviewing their company's account statements, and time spent on the phone with financial institutions. ¶¶ 78-81 (PageID 17-18). Plaintiff Finesse, in particular, has spent around 15 hours addressing the data breach, including responding to fraudulent transactions that occurred immediately following the TQL breach, which cost Plaintiff Finesse a business opportunity worth approximately $2,500. ¶¶ 78-80 (PageID 17-18). Such allegations of damages are specific, concrete, and non-speculative. *See McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019) ("The Plaintiffs have provided factual information that demonstrates that they have lost time and money as a result of taking steps to protect their personal data and prevent the misuse of that data by scammers."); *Bass*, 394 F. Supp. 3d at 1039 (allegation of loss of time responding to data breach sufficiently alleged damages for negligence claim); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at *4 ("Increased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by others courts to be specific, concrete, and non-speculative."); *cf. Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388-89 (6th Cir. 2016) ("[T]he complaints allege that Plaintiffs and the other putative class members

must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts.… [T]hese costs are a concrete injury suffered to mitigate an imminent harm[.]").

In addition, each Plaintiff sufficiently alleges redressable damages due to the diminution of their confidential information and the lost benefit of their bargain. ¶¶ 31-49, 131 (PageID 8-12, 29); *see In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953 (N.D. Cal. 2016), ("[C]ase law within the data breach context confirms that benefit of the bargain damages represent economic injury"); *see, e.g.*, *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014) (finding it plausible "that a company's security practices have economic value" and finding that plaintiffs had "plausibly pleaded" benefit of the bargain losses where defendant allegedly failed to provide adequate security); *In re Anthem, Inc. Data Breach Litig*., 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (finding allegations that plaintiffs' personal information is a "valuable commodity" and theft of this information reduces its value sufficient to plead damages for a breach of contract claim).

Defendant's reliance on *Pruchnicki v. Envision Healthcare Corp.*, No. 2:19-CV-1193-JCM, 2020 WL 853516 (D. Nev. Feb. 20, 2020) is unpersuasive. In *Pruchnicki*, the plaintiff had not alleged an actual fraudulent transaction, nor had plaintiff alleged any out-of-pocket expenses. *Id.* at *4. Here, however, Plaintiff Finesse has alleged fraudulent transactions, and both Plaintiffs have alleged that the time spent responding to the data breach has resulted in lost *company* time, with Plaintiff Finesse even missing out on a business opportunity worth approximately $2,500. ¶¶ 78-80 (PageID 17-18). In light of these significant factual differences, *Pruchnicki's* narrow holding is inapposite and fails to overcome the numerous cases that have found allegations similar to Plaintiffs' to be sufficiently concrete at the pleading stage. *See, e.g., McKenzie v. Allconnect,*

Inc., 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019); *Bass*, 394 F. Supp. 3d at 1039; *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at *4.

D. Plaintiffs Sufficiently Plead Unjust Enrichment

It is accepted doctrine under Ohio law that an action in unjust enrichment "will lie when a party retains money or benefits which in justice and equity belong to another." *Liberty Mut. Ins. Co. v. Indus. Comm'n of Ohio*, 40 Ohio St. 3d 109, 110-11 (Ohio 1988). The elements of an unjust enrichment claim are as follows: "(1) a benefit conferred by a plaintiff upon a defendant; (2) knowledge by the defendant of the benefit; and (3) retention of the benefit by the defendant under circumstances where it would be unjust to do so without payment." *Telephone Mgmt. Corp. v. Goodyear Tire & Rubber Co.*, 32 F. Supp. 2d 960, 972 (N.D. Ohio 1998).

Here, Plaintiffs have plausibly alleged the elements of an unjust enrichment claim: (i) Plaintiffs conferred monetary benefits upon TQL, including brokerage fees premised in part upon the confidentiality agreement entered into by the Parties, (ii) TQL had knowledge of and accepted these benefits, and (iii) TQL retained these benefits, despite its alleged decision to profit from those benefits by cutting costs on data security rather than to provide the necessary security to protect Plaintiffs' sensitive information. ¶ 130 (PageID 29). Thus, TQL has been unjustly enriched.

While TQL argues that an unjust enrichment claim requires that the defendant "retained the benefit of the bargain without delivering on the promise" (Def. Mtn. at 29 (quoting *Phillips v. Philip Morris Cos. Inc.*, 298 F.R.D. 355, 364 n.10 (N.D. Ohio 2014)), this argument does little to aid Defendant and, in fact, supports Plaintiffs' position. Quite simply: (1) Defendant failed to deliver on its promises to keep Plaintiffs' sensitive financial information confidential; and (2) Defendant has unjustly retained all of the profits it received, despite failing to maintain Plaintiffs' sensitive financial information confidential. Thus, Plaintiffs did not receive the full benefit of the bargain they made with TQL. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012)

(finding unjust enrichment claim sufficient based on argument that "part of which [plaintiffs] intended to pay for the administrative costs of data security," which defendant did not provide); *Cain v. Redbox Automated Retail, LLC*, 981 F. Supp. 2d 674, 687 (E.D. Mich. 2013) (finding that the plaintiffs sufficiently alleged "that they didn't receive the full benefit of their bargain" by alleging that they suffered monetary harm because "a portion of the price of each Redbox rental paid for by Plaintiffs ... was intended to ensure the confidentiality of Plaintiffs' [information]"); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at *6 (finding that plaintiffs sufficiently pled unjust enrichment claim in data breach case). Accordingly, Plaintiffs' unjust enrichment claim is plausibly alleged.

While Defendant argues that Plaintiffs cannot plead both a breach of contract claim and an unjust enrichment claim, the Federal Rules of Civil Procedure contrarily establish that a party may set out two or more statements of a claim alternatively or hypothetically, as Plaintiffs have done here. ¶ 127 (PageID 28). If a party makes alternative statements, the pleading is sufficient if any one of them is sufficient. Fed. R. Civ. P. 8(E)(2). In *Cristino v. Bur. of Workers' Comp.*, 977 N.E.2d 742 (Ohio Ct. App. 2012), the court reversed the district court's dismissal of plaintiff's unjust enrichment claim, reasoning that "[b]ecause alternative pleading is permissible, a party may plead both a breach-of-contract claim and an unjust-enrichment claim without negating the validity of either claim." *Id.* at 753; *see also Bldg. Indus. Consultants, Inc. v. 3M Parkway, Inc.*, 911 N.E.2d 356, 362 (Ohio Ct. App. 2009) ("While it is true that a party may not recover for the same services under both a contractual claim and a claim for [unjust enrichment], a party is not barred from seeking alternative theories and recovering under a[n] [unjust-enrichment] theory if his contractual claim fails."); *accord Advanced Travel Nurses, L.L.C. v. Watson*, 2d Dist. No. 24628, 2012-Ohio-3107, 2012 WL 2630431, at *11 (Ohio Ct. App. 2012). "The mere presence of both claims in a

complaint does not warrant the dismissal of the unjust-enrichment claim on a Civ. R. 12(B)(6) motion." *Cristino*, 977 N.E.2d at 753.

Because Plaintiffs' unjust enrichment claim is sufficient and because the Federal Rules of Civil Procedure and established Ohio law permit the pleading of both a contractual claim and a claim for unjust enrichment, this Court should deny Defendant's motion to dismiss Plaintiffs' unjust enrichment claim.

E. Declaratory Judgment and Injunctive Relief Claims Should Survive

Courts have discretion whether to entertain Declaratory Judgment claims. *See* Def. Mtn. at 31 (citing *Miami Valley Mobile Health Servs., Inc. v. ExamOne Worldwide, Inc.*, 852 F. Supp. 2d 925, 938 (S.D. Ohio 2012)). "[D]eclaratory relief is appropriate where a breach of contract claim will not settle all of the contractual issues concerning which plaintiff seeks declaratory relief." *Vascular Imaging v. Digirad Corp.*, 401 F. Supp. 3d 1005, 1010 (S.D. Cal. 2019).

Here, the contract that exists between Plaintiffs and TQL *specifically provides* Plaintiffs with a right to "an injunction restraining the violating Party from further violation" in the event that the confidentiality of Plaintiffs' confidential information is disclosed. The confidentiality provision provides:

> ***If confidentiality is breached***, the Parties agree that the remedy at law, including monetary damages, may be inadequate and that ***the Parties shall be entitled***, in addition to any other remedy available, ***to an injunction restraining the violating Party from further violation*** of this Agreement.

¶61 (PageID 15) (emphasis added). Thus, Plaintiffs have plausibly alleged that they are entitled to an injunction as a matter of contractual right.

Plaintiffs allege that TQL's post-breach security measures are still inadequate and request appropriate declaratory and injunctive relief to protect Plaintiffs from future injury. ¶¶ 134-41 (PageID 29-32). In its Motion, TQL admits that it does not believe it is required to implement

reasonable industry standards to protect Plaintiffs' confidential information and further claims that the confidentiality provision imposes no obligation upon it to "protect the Confidential Information of Plaintiffs and the Class." *See* Def. Mtn. at 20 (PageID 121). Thus, Plaintiffs have plausibly alleged that without an injunctive and declaratory relief they face a significant risk of being harmed again from TQL's inadequately secure IT system that still contains their confidential information. *See In re Adobe Sys.*, 66 F. Supp. 3d at 1222-23 ("Plaintiffs seek a declaration clarifying Adobe's *ongoing* contractual obligation to provide reasonable security. Plaintiffs' claim thus requests precisely the type of relief that the Declaratory Judgment Act is supposed to provide: a declaration that will prevent future harm from ongoing and future violations before the harm occurs."); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1139 (N.D. Cal. 2018) (allowing declaratory relief to proceed in data breach case); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1161 (D. Minn. 2014) ("Plaintiffs have plausibly pled that their injuries will be redressed by the injunctive relief they seek, and at this stage, that is all that is required.").

Because Plaintiffs have a contractual and factual basis for injunctive and declaratory relief, dismissal is not warranted.

V. PLAINTIFFS' CLASS ALLEGATIONS SHOULD NOT BE STRICKEN

Defendants attempt to rush the court into a determination of class certification before Plaintiffs have had the benefit of discovery and before Plaintiffs have had an opportunity to present their proposed class definition or structure. This drastic tactic by Defendant should be rejected. Indeed, "courts should exercise caution when striking class action allegations based solely on the pleadings, because class determination generally involves considerations that are enmeshed in the factual and legal issues comprising the plaintiff's cause of action." *Sauter v. CVS Pharmacy, Inc.*, No. 2:13-CV-846, 2014 WL 1814076, at *2 (S.D. Ohio May 7, 2014).

A court should only strike class allegations prior to completion of discovery when: "(1) the complaint itself demonstrates the requirements for maintaining a class action cannot be met, and (2) further discovery will not alter the central defect in the class claim." *Amerine v. Ocwen Loan Servicing LLC*, No. 2:14-CV-15, 2015 WL 10906068, at *2 (S.D. Ohio Mar. 31, 2015); *see Colley v. Procter & Gamble Co.*, No. 1:16-CV-918, 2016 WL 5791658, at *2 (S.D. Ohio Oct. 4, 2016) (explaining that in order for a court to "strike class action allegations *before* a motion for class certification[,]…the complaint itself [must] demonstrate[] that the requirements for maintaining a class action cannot be met.") (emphasis in original). These unusual circumstances simply do not exist in the present case.

A. Because Both Parties Agree that Ohio Law Applies to the Class Claims, Defendant Fails to Demonstrate a Lack of Predominance

Defendant's argument that a class action cannot be maintained due to lack of predominance is premised on Defendant's wrong assumption that "the Court—and, ultimately, the jury—will have to sift through and evaluate the common law of virtually every state if the class allegations are not struck." Def. Mtn. at 42. However, Ohio law applies to Plaintiffs' class claims. Thus, Plaintiffs' claims are appropriate for litigation as a class action.

As the Sixth Circuit has held, "[w]e generally apply the substantive law of the forum state to actions brought pursuant to our diversity jurisdiction." *Savedoff v. Access Grp., Inc.*, 524 F.3d 754, 762 (6th Cir. 2008). The application of Ohio law is further supported by the fact that each BCA with TQL contains an Ohio choice of law provision, as Defendant acknowledges. *See* Def. Mtn. at 18 (PageID 119); *see also id.* at 2 (PageID 103) ("The BCAs between TQL and Plaintiffs are 'substantially the same'"). Indeed, both Plaintiffs and Defendant agree that Ohio law applies to all claims alleged in the Complaint. *See* Def. Mtn. at 18 (PageID 119) ("Ohio Law Governs Plaintiffs' Claims"); *see also supra* at Section IV.A.

Because the claims are governed by Ohio law, TQL's defenses will likewise be governed by Ohio law. As such, Defendant's contention that its defenses will implicate a variety of laws is simply incorrect. *See* Def. Mtn. at 39-40 (PageID 137-38).

Defendant has failed to establish that individualized questions will predominate. Differences in law do not predominate because the claims brought against TQL are governed by Ohio law (as Defendant conceded).[4] Differences in fact do not predominate because the TQL data breach is derived from the same causal nexus or event, and the injury suffered is substantially similar. As such, there is no defect in the class claims that warrants striking the class allegations at the pleading stage. *Cf. Rikos v. Procter & Gamble Co.*, 799 F.3d 497, 521 (6th Cir. 2015) (rejecting argument that plaintiffs must produce actual proof at the class-certification stage of class-wide injury).

Plaintiffs have adequately pled the existence of predominance sufficient to proceed to discovery and a motion for class certification.

B. Defendant Fails to Demonstrate a Lack of Commonality

Defendant argues that Plaintiffs' allegations are incapable of being maintained as a class action because, according to Defendant, Plaintiffs cannot demonstrate commonality. To support its position, Defendant presents emails to argue that members of the alleged class were not similarly harmed in the data breach. This tactic fails.

[4] The cases relied upon by Defendant are inapposite and address concerns that are not the present in Plaintiffs' class claims. *See, e.g., Colley*, 2016 WL 5791658 at *3-4 (where plaintiffs alleged personal injury and medical-related injuries and brought common law claims "as well as *state-specific products liability claims under 23 different state statutes*," the court found class certification untenable "because Plaintiffs seek to assert these *already fact intensive claims* under the *substantive law of many different states*").

1. The Inconclusive Evidence Should Not Be Accepted as a Basis for Striking the Class Allegations

First, while a court can take judicial notice of *certain* documents at the motion to dismiss stage, it is highly questionable whether the Court can take judicial notice of the non-public TQL emails presented by Defendant (*see* Def. Mtn. at Ex. A-1, PageID 142-146). *Passa v. City of Columbus*, 123 F. App'x 694, 697-98 (6th Cir. 2005) ("[I]n general a court may only take judicial notice of a public record whose existence or contents prove facts whose accuracy cannot reasonably be questioned.") (citing FED. R. EVID. 201(b)(2)). Indeed, when the Sixth Circuit considered whether the district court properly took judicial notice of a posting on a government website, the Court held that "since the stated purpose of the Check Resolution Program is a fact whose accuracy *can* reasonably be questioned, it was not appropriate for the district court to take the City Attorney's Office's statements on its website into account when resolving the motion to dismiss without also converting the motion into one for summary judgment." *Id.* (emphasis in original). Further, even if the Court can take judicial notice of these emails, it is certainly *not* permissible for the Court to accept the contents of these emails as true. *Id.* (explaining that taking judicial notice of "documents is proper only for the fact of the documents' existence, and *not for the truth of the matters asserted therein*").

Second, even if the Court were to accept the non-public documents presented by Defendant, these documents do not refute commonality. Indeed, Defendant proffered two emails with ambiguous language sent to a purported customer. In the first email, TQL asserts that "the information that *may be* compromised *might have included* customer email addresses, phone numbers, first and last names, and TQL customer ID numbers." *See* Def. Mtn. at Ex. A-1, PageID 143-146. There is an astonishing amount of uncertainty in this email since it merely says that the exposed customer information "*included*" certain categories of information without committing to

say that the information exposed was *restricted* to these categories. The second email is similarly vague. *See id.* ("Information *possibly* obtained *might include*…."). It is, therefore, unclear from these purported emails exactly what confidential information was compromised in the TQL breach. Indeed, the very fact that TQL provided notice of the data breach to its customers suggests that the breach exposed at least something confidential as to customer information since Ohio law only requires notification of a data breach when it is "reasonably believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property." Ohio Rev. Code § 1349.19(A)(1)(a). Quite simply, while Defendant prematurely presents two purported customer emails and requests that the Court strike Plaintiffs' class allegations, these emails fail to demonstrate that Plaintiffs' class allegations should be stricken.

Regardless, to the extent freight customers did not have confidential information disclosed in the TQL data breach, this is precisely the type of factual information that will be gathered by Plaintiffs in discovery and that will inform Plaintiffs' proposed class definition and structure at the class certification stage. *See Colley*, 2016 WL 5791658, at *2 (S.D. Ohio Oct. 4, 2016) ("'[A] district court should defer decision on class certification issues and allow discovery' if the existing record is inadequate for resolving the relevant issues.'"); *Pilgrim v. Universal Health Card, LLC*, 660 F.3d 943, 949 (6th Cir. 2011) ("A court may properly strike class allegations prior to discovery where discovery would not have "alter[ed] the central defect in th[e] class claim.").

2. Commonality Exists as to Plaintiffs' Class Allegations

As this Court has explained, "class certification will not be denied simply because the class members' claims have some factual dissimilarities.' The most important consideration, rather, is whether there exists "*a common element of fact or law*" among the claims." in *Amerine v. Ocwen Loan Servicing LLC*, No. 2:14-CV-15, 2015 WL 10906068, *4-5 (S.D. Ohio Mar. 31, 2015).

Here, there are several common questions of fact or law, including whether TQL utilized adequate security measures to reasonably secure class members' confidential information. ¶ 95 (PageID 20-22). Answering this question will ultimately turn on the same evidence of the protocols and procedures that TQL used to safeguard class members' data. For this very reason, courts have overwhelmingly found that data breach claims, like those presented here, are especially well-suited for class treatment. *See In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 316 (N.D. Cal. 2018) ("[T]he predominant issue in this case is whether Anthem properly secured the personal information taken from its data warehouse. That question can be resolved using the same evidence for all Settlement Class Members.") (collecting cases); *Hutton v. Nat'l Bd. Of Exam'rs in Optometry, Inc.*, 2019 WL 3183651, *4 (D. Md. July 15, 2019) ("[P]otential damages suffered by individual class members are relatively low-dollar amounts and would be uneconomical to pursue on an individual basis given the burden and expense of prosecuting individual claims.").

That there *may* have been two different types of data exposed in the breach, does not change this. As the Sixth Circuit in *Rikos* held:

> The key point at the class-certification stage is that this kind of dueling…evidence *will apply classwide* such that individual issues will not predominate. In other words, assessing this evidence will generate a *common answer* for the class based on Plaintiffs' theory of liability—whether Align in fact has been proven scientifically to provide digestive health benefits for anyone. That common answer, of course, *may be that Align does work for some subsets of the class*. That does *not* transform this classwide evidence into individualized evidence that precludes class certification, however. Neither P & G nor the dissent has articulated how evidence that Align might work for some sub-populations actually would necessitate individualized mini-trials that should preclude class certification. Rather, the more straightforward impact of this evidence is simply that it may prevent Plaintiffs from succeeding *on the merits*.

799 F.3d at 520.

The risk of individualized mini-trials is notably far less likely here than it was even in *Rikos*. Indeed, Defendant's contention is that the *entire group of customers* had different data

exposed in the breach. Thus, even accepting Defendant's premature assertion as true, the categories of confidential information exposed can be broken into two *broad* groups: (1) motor carriers, and (2) customers. This can easily be addressed on a class-wide basis whether by establishing a subclass for customers, by having two damage models, or otherwise. The Complaint provides that the alleged class definition may be amended or refined. ¶ 89 (PageID 19). This statement was not superfluous. At the class certification stage, Plaintiffs will have information collected from discovery that will inform how Plaintiffs propose a class, including whether Plaintiffs propose a more defined class or subclasses to address potential distinctions. *See Amerine*, 2015 WL 10906068, at *2 (explaining that a court should *only* strike class allegations prior to the close of discovery if further discovery would "not alter the central defect in the class claim"). Thus, even to the extent Defendant is right in its premature assertion that the entire group of customers were "uninjured" in TQL's data breach, this would not create disparate factual issues to prevent class certification but would have "the more straightforward impact" of preventing the customer group "from succeeding *on the merits*." *Rikos v. Procter & Gamble Co.*, 799 F.3d 497, 521 (6th Cir. 2015); *see id.* ("Rule 23(b)(3) requires a showing that *questions* common to the class predominate, not that those questions will be answered, on the merits, in favor of the class.") (emphasis in original).

Defendant has failed to demonstrate that Plaintiffs' class action cannot be maintained, such that the class allegations should be stricken. *Amerine*, 2015 WL 10906068, at *5 ("[T]he action of striking portions of a pleading, especially entire causes of action, is a 'drastic remedy' that should be used with caution."). To the extent remaining questions exist as to whether Plaintiffs' claims are capable to proceeding as a class action, such questions should be resolved following discovery and Plaintiffs' motion seeking class certification.

VI. CONCLUSION

For the reasons stated herein, Plaintiffs respectfully request that the Court deny Defendant's Motion in its entirety. In the event the Court dismisses the Complaint in whole or in part, Plaintiffs respectfully request leave to amend. *See* Fed. R. Civ. P. 15(a)(2) (leave to amend shall be "freely" given); *Tefft v. Seward*, 689 F.2d 637, 639 (6th Cir. 1982) (holding that Rule 15(a) creates a liberal policy in favor of granting leave to amend and is meant to "reinforce the principle that cases should be tried on their merits rather than the technicalities of pleadings").

Date: June 22, 2020

By: */s/ William B. Federman*
William B. Federman (*Admitted Pro Hac Vice)*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Marc E. Dann (0039425)
Brian D. Flick (0081605)
DANN LAW
P.O. Box 6031040
Cleveland, Ohio 44013
(216) 373-0539
(216) 373-0536 facsimile
notices@dannlaw.com

Cornelius P. Dukelow (*Admitted Pro Hac Vice)*
Abington Cole + Ellery
320 South Boston Avenue, Suite 1130
Tulsa, OK 74103
Telephone and Facsimile: (918) 588-3400
cdukelow@abingtonlaw.com

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I certify that on June 22, 2020, this document was electronically filed with the Clerk of Court using the CM/ECF system, which will serve a true and exact copy of the filing to counsel of record, including:

Matthew J. Wiles (0075455)
Sara H. Jodka (0076289)
Jordan D. Rauch (0093389)
DICKINSON WRIGHT PLLC
150 E. Gay Street, 24th Floor
Columbus, Ohio 43215
Telephone: (614) 744-2570
mwiles@dickinsonwright.com
sjodka@dickinsonwright.com
jrauch@dickinsonwright.com

Attorneys for Defendant
Total Quality Logistics, LLC

/s/ William B. Federman
William B. Federman
Federman & Sherwood